WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

December 26, 2018

Anjali C Das
312.821.6164 (direct)
708.990.2417 (mobile)
Anjali.Das@wilsonelser.com

Attorney General Xavier Becerra
Office of the Attorney General
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Data Security Incident

Dear Attorney General Becerra:

We represent MJ Insurance ("MJ"), located in Indianapolis Indiana, and Phoenix, Arizona, with respect to a potential data security incident described in more detail below. MJ takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On September 26, 2018, MJ was alerted that an unknown individual potentially gained access to one of its employee's e-mail account. It appears that the employee may have been the victim of an email phishing campaign. Upon discovering the incident, MJ immediately took action and notified its IT department of the incident, who prevented any further unauthorized access by changing the employee's password and email credentials. MJ also retained an independent computer forensics company to conduct an extensive IT investigation to determine what information may have been accessed. The investigation confirmed that the incident was limited to one employee's email account, and that no other systems or servers were impacted. On November 26, 2018, based on the results of the lengthy, detailed forensics investigation, MJ confirmed that the e-mail account contained personally identifiable information, including first and last names, dates of birth, driver's license numbers and/or Social Security number. No financial account information was involved in this incident.

2. Number of California residents affected.

A total of one thousand seven hundred and thirty-two (1,732) residents of California were potentially affected by this security incident. Notification letters to these individuals were mailed on December 26, 2018, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

MJ has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially impacted individuals' information. This includes providing potentially affected individuals with complimentary credit monitoring and identity theft restoration services, along with strengthening its cybersecurity posture by enabling multi-factor authentication for access to email accounts, and implemented longer and additional password requirements to improve password strength. In addition, MJ is enforcing stricter cybersecurity reeducation timelines for all users, and reviewing record retention rules to ensure information is not kept any longer than necessary. MJ is also providing potentially impacted individuals with identity theft restoration and credit monitoring services for a period of twelve (12) months, at its own expense, through CyberScout.

4. Contact information.

MJ remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das SF

Enclosure

Cc: California Department of Insurance
Attn: Susan Bernard, Division Chief, Field Examinations
45 Fremont Street, 24th Floor
San Francisco, CA 94105
Email: susan.bernard@insurance.ca.gov

O 602 772 3300 F 602 772 3349
A 3900 E. CAMELBACK RD., SUITE 225, PHOENIX, AZ 85018
W MJINSURANCE.COM

<<First Name>><<Last Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>><<Last Name>>:

Re: Notice of Data Breach

We are writing to inform you of a data security incident involving MJ Insurance ("MJ") that may have resulted in the disclosure of some of your personal information. At this time, we are not aware of the misuse of any of your information. Nonetheless, we are notifying you out of an abundance of caution. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident, steps you can take to protect your information, and resources we are making available to help you.

What happened and what information was involved:

MJ is an independent insurance agency with offices in Indiana and Arizona. On September 26, 2018, we discovered that an unknown individual gained access to one of our employee's e-mail accounts. It appears that our employee may have been the victim of an email phishing campaign. The employee's account contained stored e-mails that may have included some of your personally identifiable information ("PII") including your name, date of birth, driver's license number and/or Social Security number. We note that no financial account information was involved in this incident. Although we are not aware that any of your personal information was taken, we are notifying you on the basis that some of your information was contained in the employee's email account. If you have not worked with MJ directly, we may have obtained limited information about you through one of the employers to whom we provide employee benefits consulting and support services.

Upon discovering the incident, our IT department immediately prevented any further unauthorized access to the account by changing the employee's password and email credentials. We also retained an independent computer forensics company to conduct an extensive IT investigation to determine what information may have been accessed. The investigation confirmed that the incident was limited to one employee's email account, and that no other systems or servers were impacted. The lengthy, detailed investigation also revealed that some of your information was contained in the email account at issue. However, the investigators did not find evidence that your information was in fact stolen or misused.

What we are doing and what you can do:

As a precautionary measure, we are providing you with complimentary resources to help protect your identity. We have secured the services of CyberScout, a company specializing in identity theft education and resolution, to provide you with fraud resolution support, including identity theft restoration services, and access to *Single Bureau Credit Monitoring*[1] services and at no charge to you for a period of twelve (12) months from the date of enrollment. With this protection, CyberScout will provide you with alerts when changes occur to your Experian credit file and will help you resolve issues if your identity is compromised due to this incident. These alerts are sent to you the same day that the change or update takes place with the bureau.

How do I enroll for the free services?

To enroll in Credit Monitoring* services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE.>

[1]Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For guidance with the CyberScout services, or to obtain additional information about these services, please call the CyberScout help line *1-800-405-6108* and supply the fraud specialist with your unique code.

We are committed to ensuring security of all information in our control, and are taking steps to prevent a similar event from occurring in the future. This includes, strengthening our cybersecurity posture by enabling multi-factor authentication for access to email accounts and reviewing our record retention rules to ensure information is not kept any longer than necessary.

For more information:

Please know that the protection of your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-855-652-4700, Monday through Friday, 8:00 am to 5:00 pm Eastern Time.

Sincerely,

Michael H. Bill
Chief Executive Officer

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:
You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf) or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.